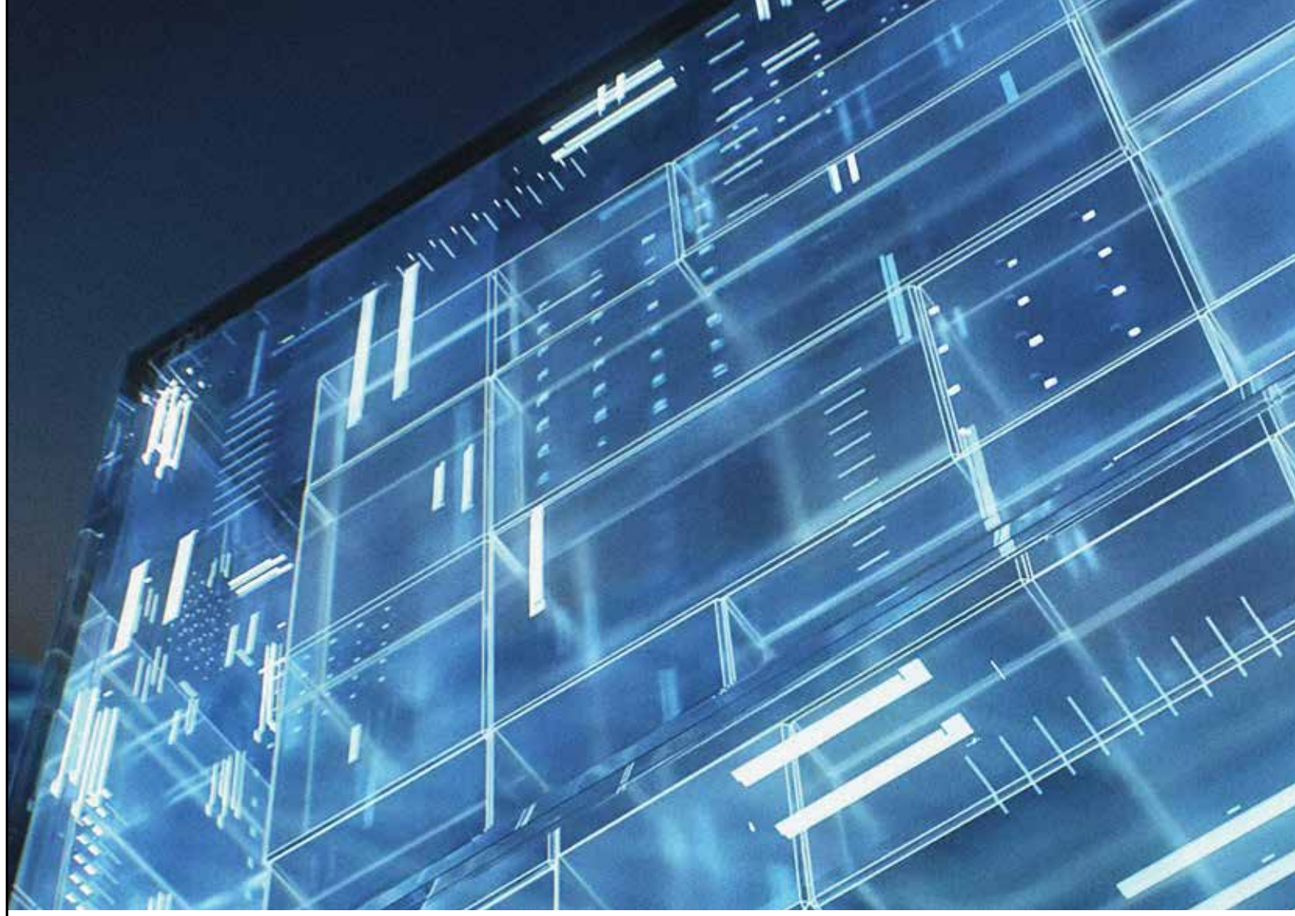
A propos de Kaspersky

Kaspersky est une entreprise internationale de cybersécurité fondée en 1997. L'expertise de Kaspersky en matière de sécurité et de **threat intelligence** est constamment transformée en solutions et services de sécurité pour protéger les acteurs publics comme privés ainsi que les consommateurs à travers le monde. La gamme de produits de sécurité de Kaspersky comprend des solutions de protection des terminaux et des solutions et services de sécurité spécialisés pour lutter contre les menaces numériques sophistiquées et en constante évolution. Plus de 400 millions d'utilisateurs sont protégés par les technologies Kaspersky et nous aidons 270 000 entreprises à protéger ce qui compte le plus pour elles.

Pour en savoir plus :
www.kaspersky.com/
www.kaspersky.com/transparency-center
https://www.kaspersky.com/transparency-center-offices

www.kaspersky.com

kaspersky



Appel de Paris pour la Confiance et la Sécurité dans le Cyberespace

La proposition de Kaspersky pour soutenir et concrétiser les initiatives nées de l'Appel de Paris

Novembre 2019

Proven.
Transparent.
Independent.

kaspersky BRING ON THE FUTURE

En savoir plus
www.kaspersky.com

Appel de Paris pour la Confiance et la Sécurité dans le Cyberespace

Kaspersky soutient pleinement l'Appel de Paris lancé par le Président Emmanuel Macron le 12 novembre 2018 pour renforcer la confiance, la sécurité et la stabilité dans le cyberespace. Au regard de la place croissante qu'occupent les technologies numériques dans nos vies, nous sommes fermement convaincus que la cybersécurité doit venir compléter la numérisation de la société afin d'assurer la sûreté et la sécurité des citoyens.

En réponse à l'Appel de Paris, qui encourage la collaboration entre les pouvoirs publics, le secteur privé et la société civile pour renforcer la cyberprotection, et en tant que l'un des premiers signataires de l'Appel, nous souhaitons présenter ici nos pistes de réflexion pour concrétiser, ensemble, les idées et les valeurs portées par cette initiative.

Définir ensemble les conditions de la confiance

L'Appel de Paris réunit tous les acteurs – experts de l'industrie, monde universitaire, secteur public et société civile – pour élaborer ensemble un cadre global partagé.

Un tel cadre, qui prendrait en compte les risques tout au long de la chaîne d'approvisionnement informatique, permettrait de définir les conditions que doivent respecter les produits informatiques pour mériter notre confiance (évaluer leur « trustworthiness »). Il aiderait ainsi toutes les parties prenantes – particuliers, entreprises, autorités publiques – à accorder sereinement cette confiance.

Kaspersky propose de fournir son infrastructure et ses systèmes, y compris son code source, pour les évaluations nécessaires au bon fonctionnement du cadre (voir ci-dessous).

Deux éléments doivent être étudiés en priorité :

- **Évaluation de l'intégrité des produits** : Un produit informatique ne contient-il pas de fonctionnalités imprévues ?
- **Évaluation de la collecte et du traitement des données** : Comment un produit informatique collecte, traite, stocke et protège les données des utilisateurs ?

Pour renforcer la coopération sous l'égide de l'Appel de Paris, nous soutenons également les idées suivantes :

- **La création d'une plateforme collaborative** avec des rencontres physiques pour recueillir des idées et créer une coopération simplifiée entre les signataires de l'Appel. Un tel dispositif rationalisé pourrait se concentrer sur l'élaboration (i) d'un cadre de confiance ; (ii) de normes cyber ; (iii) de cyber « hygiène » et pédagogie.
- **La mise en place d'un mécanisme de consultation** avec des rencontres physiques pour l'élaboration d'une approche et d'un cadre de normalisation des produits de cybersécurité.
- **Une publication multipartite** pour partager les réflexions sur les mesures possibles pour promouvoir les valeurs et atteindre les objectifs de l'Appel.

La légitimité du cadre et son acceptabilité, mais aussi la mutualisation entre acteurs et le partage de compétences, seront des enjeux clés pour la réussite de telles initiatives. Kaspersky est prêt à s'engager aux côtés des signataires de l'Appel de Paris.

Paradigme de la « Confiance Rationnelle » (Verifiable Trust)

L'importance de la confiance dans le domaine de la cybersécurité

Nous accordons tous une place majeure à la confiance dans nos relations humaines et professionnelles. Dans le domaine de la cybersécurité, la confiance est encore plus importante : en effet, la cybersécurité ne s'appuie pas seulement sur la confiance mais en dépend entièrement. La confiance, en matière numérique, se définit comme la combinaison de la cybersécurité, de la protection efficace des données, de la responsabilité et la traçabilité, ainsi que du traitement éthique, inspirant la confiance des clients envers une entreprise – ou des citoyens envers un acteur public.

Les travaux et réflexions en cours à l'échelle internationale, pour encadrer par le droit les comportements dans le cyberespace, doivent permettre aux acteurs des relations internationales d'en faire un lieu sûr et sécurisé, de renforcer la cyberstabilité et contribuer ainsi à rendre le monde moins chaotique. Nous sommes de fervents partisans de toutes ces initiatives. Cependant, nous sommes également conscients que cela nécessitera encore beaucoup d'efforts, de temps et une forte volonté de la part des États pour créer les conditions d'application nécessaires au respect de ces normes. En outre, ces initiatives laissent souvent de côté les acteurs non-étatiques qui restent dans une « zone grise » juridique. A titre d'exemple, le principal objectif du rapport du Groupe d'Experts Gouvernementaux (GGE) de l'ONU en 2015 était « d'accroître la stabilité et la sécurité dans l'environnement mondial des TIC », en identifiant « de nouvelles normes volontaires et non-contraignantes pour un comportement responsable des États ».

Ainsi, alors que les discussions se poursuivent au sein des instances internationales, Kaspersky souhaite proposer des solutions concrètes pour renforcer la confiance numérique et la cyber-immunité face aux nouvelles cybermenaces. L'industrie de la cybersécurité a besoin d'un cadre mondial pour la confiance et l'intégrité qui s'applique à tous. La **transparence** en est la pierre angulaire.

Généralement, la confiance dans une entreprise est fondée en grande partie sur sa réputation, sur la relation construite au long terme avec ses publics. La décision de faire confiance ou non repose donc sur l'opinion personnelle de chacun, sur la base de son expérience passée, de sa culture et de ses valeurs. Une confiance basée sur le référentiel de chacun peut être à géométrie variable et s'appuyer sur la peur de risques potentiels.

Dans le domaine technique et stratégique que représente le numérique, ne conviendrait-il pas de **réfléchir à une nouvelle approche qui serait davantage fondée sur des données probantes plutôt que sur des impressions** ? Ceci afin d'élaborer un cadre commun, un standard de référence en cybersécurité assurant un niveau de protection minimum à l'échelle mondiale.

Nous devons aujourd'hui changer de paradigme pour que la décision de faire confiance soit construite sur une réflexion factuelle voire « scientifique ». Pour y parvenir, il est nécessaire d'élaborer un nouveau cadre, d'instaurer un nouvel état d'esprit régi par les principes de confiance et d'éthique numériques, qui seraient fondés sur une approche effective et claire de l'évaluation des risques.

La Global Transparency Initiative Une démarche unique d'indépendance et de transparence pour la confiance numérique

La GTI offre aux organisations des outils concrets pour s'assurer que les solutions Kaspersky respectent ou vont au-delà des politiques de sécurité, de protection et de gestion des données d'entreprise. Un effort qui s'inscrit dans la durée, car la confiance n'est jamais entièrement acquise : elle doit constamment être renouvelée.

Nous sommes aujourd'hui convaincus que la GTI pourrait devenir un modèle pour le secteur, et permettrait de contribuer au renforcement de la confiance à l'ère numérique.

GTI : Les 4 piliers de la confiance

1. Gestion des données
- Délocalisation du traitement et du stockage des données en Suisse, un pays où la réglementation en matière de protection des données est très stricte,
- Élaboration de réseaux cloud privés avec le plus haut niveau de confidentialité (Kaspersky Private Security Network).

2. Vérification – Fiabilité
- Ouverture de centres de transparence pour l'analyse du code source Kaspersky, des mises à jour de logiciels et règles de détection des menaces,
- Gestion des vulnérabilités par le biais du programme continu Bug Bounty,
- Performance et efficacité maximales basées sur les résultats de plus de 70 tests,
- Évaluation indépendante des clients – Gartner Peer Insight.

3. Intégrité
- Évaluation de l'intégrité et de la sécurité du développement du logiciel Kaspersky par un audit indépendant SOC 2 effectué par l'un des quatre grands cabinets comptables. L'audit a conclu que le développement et la publication des bases antivirus de Kaspersky sont protégés contre les modifications non autorisées grâce à des contrôles de sécurité rigoureux ;
- Développement de projets collaboratifs avec le milieu universitaire et des tierces parties pour asseoir ce cadre de confiance numérique.

4. Culture d'entreprise
- Indépendance : Kaspersky, une société privée avec plus de 22 ans d'expérience,
- ADN de l'entreprise : développement continu de nouvelles technologies,
- Recherche : Global Research and Analysis Team (GReAT), un tiers des employés sont des spécialistes en R&D,
- Partage d'expérience : le Security Analysts Summit, une conférence mondiale phare pour les experts en cybersécurité.

La transparence, la sécurité et la confidentialité des données sont des éléments primordiaux pour nos utilisateurs, partenaires et pour la communauté internationale de cybersécurité dans son ensemble. C'est pourquoi Kaspersky a élaboré une approche unique – the Global Transparency Initiative (GTI) – visant à renforcer la résilience de son infrastructure informatique face à tout risque, fût-il théorique, susceptible de nuire à la confiance.

En vertu de ce dispositif, **nous avons transféré le coeur de l'infrastructure de stockage et de traitement des données de nos utilisateurs européens à Zurich, en Suisse**. Ce mouvement se poursuivra pour les utilisateurs des autres régions du monde.

L'ouverture de centres de transparence à Zurich et à Madrid permet également à nos partenaires de procéder à un audit de nos produits dans un environnement sécurisé. En 2019, nous avons également annoncé l'ouverture d'un troisième centre de transparence à Kuala Lumpur, en Malaisie. Dans nos centres de transparence, nous offrons également la possibilité de construire un produit à partir de son code source et de le comparer avec celui accessible au public. Cela prouve que le code source fourni pour une révision est bien celui qui a été utilisé pour construire la version publiquement disponible du produit. Aucun autre fournisseur de cybersécurité n'a proposé une approche aussi forte.

En outre, l'audit indépendant effectué par un cabinet renommé comptant parmi les « Big Four » sur la base du référentiel SOC 2 a confirmé l'intégrité et la sécurité du développement et de la diffusion des bases de données antivirus de l'entreprise. Enfin la **prime aux « bug bounty »**, qui récompense la découverte de failles dans les programmes Kaspersky, a par ailleurs été relevée. Elle peut désormais atteindre 100 000 $ pour les vulnérabilités les plus sévères, afin d'inciter davantage les chercheurs indépendants en sécurité à compléter nos efforts de détection et d'atténuation des vulnérabilités.

Les mesures clés :

- Transfert en Suisse de toutes les données des utilisateurs européens
- Ouverture de centres de transparence à Zurich, Madrid et Kuala Lumpur dans lesquels les parties tierces peuvent auditer le code, les mises à jour et le code de compilation
- Audit SOC 2 de nos processus par un tiers indépendant membre des « Big Four »
- Relèvement de la prime « Bug bounty »